REMARKS/ARGUMENTS

Claims 1-22 were presented and examined. Claims 1-22 were rejected under 35 USC § 102(e), as being anticipated by Blumenau (USPN 6,260,120). In this response, Applicant has amended claims 6-9, 15, and 16. Claims 1-22 remain pending.

Specification Amendments

Applicant has corrected certain grammatical and typographical errors found in the specification as originally filed. Applicant believes that no new matter is introduced by these corrections. The specification amendments are made for purposes of clarity only and are not made for any purpose related to patentability.

Claim rejections under 35 USC § 102(e)

The Examiner rejected claims 1-22 under Section 102(c) as being anticipated by Blumenau.

With respect to the rejection of independent claims 1 and 19, Applicant respectfully traverses the rejection because the cited reference does not disclose all of the limitations of the claims. Specifically, Blumenau does not disclose or suggest an authentication method in which a first value is retrieved from a password table and then used to retrieve a second value from the password table. Nor does Blumenau disclose an authentication method in which, upon receiving an encrypted copy of the first value, the encrypted first value is decrypted and used to retrieve a third value from a second copy of the password table. Because Blumenau does not disclose or suggest these elements, the Section 102(e) rejection of independent claims 1 and 19 is improper.

Supporting the rejection of claims 1 and 19, the Office Action indicates that the claimed elements are disclosed in columns 39-42 of Blumenau. This portion of Blumenau teaches an authentication method in which a list of random numbers is stored on a storage subsystem port and on a host controller that will access the port. The random numbers in the list are then used to authenticate a sequence of accesses to the storage subsystem by the host controller. The first random number is used to authenticate a first access, the second random number is used to access the second random number, and so forth. With respect to each individual access, Blumenau describes an authentication method in which the current random number is sent from the port adapter to the host controller in response to an access request. The host controller encrypts the random number, using an encryption key known only to the host and the port adapter, and sends the encrypted random number to the port adapter. Meanwhile, the port adapter locally encrypts the random number using the encryption key and, upon receiving the encrypted random number from the host controller, compares the two copies of the encrypted random number. Access to the storage subsystem is authorized if the two copies match and denied otherwise.

In contrast, the present invention as recited in independent claims 1 and 19 is an authentication method in which copies of a password table are stored on a host and a storage access network (SAN) node. When the host attempts to access the SAN node, the SAN node authenticates the host by retrieving a first value from the SAN node's copy of the password table. The first value is then used to retrieve a second value (referred to as the response) from the password table. The first value is then encrypted and sent to the host, which uses the first value to retrieve the third value (which represents the host's response value) from the host's copy of the password table. The third value is then encrypted and sent back to the SAN node, which decrypts the host's response value and compares the host's response value with its own response value.

By using a first value to retrieve the second value from the password table, the present invention, as recited in claims 1 and 19, provides an additional level of security over the cited reference. Specifically, the present invention provides secure authentication not just by the use of shared copies of encryption keys and table values, but also by using the first value to select the second and third values from the password tables. One attempting to obtain authorization to the SAN node would have to know not only the encryption keys and the password tables, but also the manner in which the first value is used to obtain the second and third values from the table. Blumenau contains no such additional level of security. Persons having knowledge of the shared keys and random number lists of Blumenau have all the information they need to present the port adapter with a satisfactory response during authentication because it is the random number itself that is the entire basis for authentication in Blumenau.

Thus, Blumenau simply does not teach or suggest "using the first value to retrieve a second value from...the password table" or "using the first value to retrieve a third value from...the password table" where the first value, itself, is retrieved from the password table, all as recited in claims 1 and 19. An anticipation rejection is appropriate only when the cited reference discloses all claim limitations. See, e.g., MPEP § 2131. ("A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference.", citing *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Because claims 1 and 19 as presented contain limitations not expressly or inherently described in Blumenau, Applicant would respectfully request the Examiner to reconsider and withdraw the Section 102(e) rejection of claims 1 and 19, and all claims depending thereon.

With respect to independent claim 9, Applicant has amended to recite explicitly that the password retrieved from the password table is then used to retrieve the response from the password table. Independent claim 9, as amended, is not anticipated by Blumenau for the same reasons that originally presented claims 1 and 19 are not anticipated by Blumenau. Accordingly, Applicant would respectfully request the Examiner to reconsider and withdraw the Section 102(e) rejection of independent claim 9 as amended herein and all claims depending therefrom.

In addition to the foregoing, Applicant would respectfully submit that claim 2 as originally submitted recites limitations neither disclosed nor suggested by the cited reference. Specifically, claim 2 recites, in addition to the authentication steps recited in claim 1, an independent authentication mechanism, invoked upon system reset or power-on, in which a code derived from the host's serial identification is used to verify the corresponding host by comparing the serial-based code to a previously stored copy of the code. In this manner, the hardware identity of each host is verified following system reset to prevent the substitution of a rogue host for an authorized or known host.

The Office Action states that the limitations of claim 2 are disclosed in Blumenau at column 5 and columns 11 and 12. Applicant respectfully submits that Blumenau does not disclose or suggest the limitations of claim 2. Blumenau does describe the storage of permanent host identifiers, which may include a host's WWN (a unique identifier that may include a serial number), but Blumenau does not describe generating a code based upon the serial number and using this generated code to authenticate a hardware entity following system reset. Blumenau merely teaches that permanent identifiers have too many bits to be suitable for use in a packet or frame. Blumenau teaches that, instead, it is desirable to associate the permanent identifier with a presumably smaller temporary identifier and to use the temporary identifier in packets to identify the source and destination of each packet. See, Blumenau column 11, line 57 through column 12, line 17.

Although there is a weak and superficial analogy between the permanent / temporary identifiers of Blumenau and the serial number and corresponding code of the present invention as recited in claim 2, the analogy breaks down upon closer inspection. Blumenau, for example, does not disclose or suggest using the temporary identifier as part of an authentication mechanism following system reset. Instead, Blumenau merely describes the use of the temporary identifier to indicate the source and destination of SAN packets. Identifying source and destination address for packets is not the same as authentication. Substantially all networked packets include some form of source and destination address regardless of whether the network supports or requires authentication. Conventional HTTP requests in a web server application, for example, include source and destination IP address, but the requests are generally not authenticated. Thus, Blumenau is merely describing the use of a relatively compact identifier, which is associated with a WWN, to reduce the size of SAN packets and thereby reduce the consumption of scarce transmission bandwidth.

The (only) authentication mechanism disclosed by Blumenau is described with respect to FIG. 33 at columns 39, 40, and 41. Explicit in this description is that Blumenau uses the temporary identifiers merely to route requests. According to Blumenau, the challenge response authentication is implemented using the Fibre Channel "Exchange ID's", which are independent of the source and destination ID's. Blumenau neither teaches nor suggests any correspondence between the temporary identifiers and the exchange ID's that are used for authentication. Instead, Blumenau describes that the authentication data consists of random numbers encrypted using an encryption key known to the host and the controller. Because Blumenau does not disclose or suggest the use of host serial numbers to generate codes that are used to authenticate hosts following a system reset, Blumenau does not anticipate the limitations of claim 2. Applicant, therefore, would respectfully request the Examiner to reconsider and withdraw the rejection of dependent claim 2. Analogous arguments apply to dependent claims 16 and 20 and Applicant would request the Examiner to withdraw the rejection of these claims and all claims depending thereon.

With respect to dependent claim 3, Applicant would respectfully dissent from the Section 102(e) rejection because Blumenau does not disclose the use of a time stamp, in conjunction with a host serial number, to generate a code that is used to authenticate the host. Rejecting claim 3 as originally submitted, the Office Action indicates that Blumenau "discloses wherein the code value is further based on a time stamp and date stamp" at col. 39, lines 44-54. The cited portion of Blumenau reads as follows:

> As used in this specification, the term "random number" would include a so-called "pseudo-random number" so long as the number would appear to be selected at random during the typical duration of time that a host controller is logged in to a port adapter. For example, the random numbers transmitted by the port adapter to a host controller are generated by a conventional random number generator routine that is seeded at the time that the host controller logs in to the port adapter. The BASIC programming language, for example, provides such a random number generator routine.

Applicant is unable to determine any significant relevance between the cited portion of Blumenau and the claim under consideration. Accordingly, Applicant would respectfully request the Examiner to reconsider and withdraw the rejection of dependent claim 3. Analogous arguments apply to claim 21.

In addition to the foregoing, Applicant has amended claims 6 and 7 to recite previously unclaimed limitations. In claim 6 as amended, the retrieval of the first value from the password table is recited as including randomly accessing an entry in the password table. Support for this amendment is found in the specification as originally filed at the paragraph beginning on page 9, line 18 and, thus, no new matter is presented. This method of retrieving the password from the password table is superior to the method described in Blumenau. Whereas Blumenau simply generates a list of random numbers, which are then used in a sequential manner, randomly accessing a table of values as recited in amended claim 6 prevents an unwanted user from knowing which password or value will be used during the next authentication sequence. Blumenau, in contrast, is "predictable" in the sense that anyone in possession of the random number list knows which random number will be used during the next authentication sequence because the numbers are used sequentially.

Claim 7 as amended recites a limitation, in addition to the limitation of claim 6, wherein the first value is hashed to determine a second entry in the password table from which the second value is retrieved. Support for this amendment is found in the specification as originally filed at the paragraph beginning on page 9, line 18 and, thus, no new matter is presented. Claim 7 as amended explicitly recites that the second entry in the password, from which the second value is retrieved, is determined algorithmically from the first value. As described above with respect to claim 1, using an algorithm to determine which entry is ultimately accessed to retrieve the "response" value provides greater security by adding an additional level of knowledge to the authentication mechanism. When the manner in which the password table is accessed is derived algorithmically, such as by a hashing algorithm, mere possession of the password table is of limited if any use to hackers since they will not know which entry in the password table is significant unless they also know the hashing algorithm employed. This limitation is neither taught nor suggested by Blumenau, which merely teaches sequentially accessing a list of random numbers and encrypting the random numbers directly. Blumenau contains no teaching or suggestion, for example, to access the random number list a second time based on the value of the first random number. Accordingly, Applicant would respectfully submit that the limitations of amended claims 6 and 7 are neither taught nor suggested by the cited reference.

In this response, Applicant has addressed the claim rejections under 35 USC § 102(e), which is the only issue raised in the Office Action. Accordingly, Applicant believes that this response constitutes a complete response to the Office Action. In light of the amendments made herein and the accompanying remarks, Applicant believes that the pending claims are in condition for allowance. Accordingly, Applicant would request the Examiner to withdraw the rejections, allow the pending claims, and advance the application to issue. If the Examiner has any questions, comments, or suggestions, the undersigned attorney would welcome and encourage a telephone conference at 512.428.9872.

Respectfully submitted,

Joseph P. Lally
Reg. No. 38,947
ATTORNEY FOR APPLICANT(S)

LALLY & LALLY, L.L.P.
P.O. Box 684749
Austin, Texas 78768-4749
512.428.9870
512.428.9871 (FAX)

JPL/mmm